PUBLISHED BY
JR
EDUCATION

Available online at http://ijite.jredu.id

IJITE

International Journal of Information Technology and Education (IJITE) 1(2), (March 2022) 109 – 118

International Journal of Information Technology and Education (IJITE)

http://ijite.jredu.id

Student Information Security Awareness on the Use of ATM Machines

Trudi Komansilan[1], Sondy C. Kumajas[2], Triska Pinatik[2*]

Department of Information Technology and Communication, Universitas Negeri Manado, Indonesia

*Corresponding author : triskapinatik@gmail.com

ARTICLE INFO

Article history:

Received: 19 November 2021; Received in revised form: 29 Desember 2021; Accepted: 18 March 2022;

Available online: 17 March 2022; Handling Editor: Fabiola Natasya Wauran

ABSTRACT

This study examines literature studies on security systems at automated teller machines which include PIN security and forms of attacks on ATM security. The method used in ATM security is the use of a PIN to be able to access and make transactions through ATM machines. PIN security is carried out using a cryptographic process (encryption and decryption) using the Triple DES standard (data encryption standard). The use of ATMs is inseparable from the need to maintain a security system at ATMs. This document describes the use of DES and Triple DES cryptographic methods. Currently there are various threats that attack security in the use of ATMs such as skimming, phishing.

Keywords : Automated Teller Machine, data encryption standard, phishing

INTRODUCTION

ATM (Automated Teller Machine) is a computerized device used by a financial institution (bank) in an effort to provide financial transaction services (withdrawing money) in public places without requiring bank employees (tellers). to facilitate the service of

withdrawing money from customer savings, but along with the development of technology and the need for improved services to customers, the use of ATMs has expanded not only to withdraw money. It is now possible for customers to make money transfers, payments, balance checks, and other financial transactions simply by using an ATM. In general, ATM technology is a form of distributed computer network. ATM network The existence of transaction processing (communication) between computers through a wide network, the issue of security is an issue that needs special attention. This is of course to ensure that the transaction process can occur properly and correctly. The security technique used. ATM Security System is the use of a personal identification number (PIN) so that only certain people can access or make transactions at ATMs. For access to ATM machines, customers will have a card with a magnetic tape or a chip that functions as a place to store data such as card numbers, PIN numbers, and other security data.

In the security system applied to ATMs, there is a data encryption process to maintain the security of personal data, such as PIN numbers or card numbers, and also to maintain security during the transaction process (during the transaction process there is communication between the ATM and the bank computer through the banking net).). To ensure security at ATMs, data encryption methods with data encryption standard (DES) techniques are used; which was later developed into Triple DES in order to improve data security. Algorithm schema on DES. In the enciphering process, each round is used an algorithm with the Feistel network model. Thus in the process of enciphering the plaintext block from the initial permutation will be divided into two parts with a size of 32 bits each. It is in this Feistel network that the internal key to the transformation function is used.

ATM Security System

In DES key generation is done using the external key given previously. The internal key generation process is done by permutating and shifting bits to the left. The entire internal key generation is carried out for the deciphering (decryption) process on DES, the operation performed is the opposite of the operation performed during the ciphering process. The use of DES as a data cryptography (security) standard is still debated and in DES there is a fatal security loophole, namely the use of a 56-bit key. The use of this "low" number of keys (256 or 72,057,594,037,927,936 possibilities) makes it vulnerable to security attacks. The Electronic Frontier Foundation (EFE) in 1998 designed and built a hardware device (DES cracker) using the exhaustive search key method to crack the DES key and is expected to be able to find the DES key within 5 days. A year later, the use of DES cracker with internet collaboration can find DES keys in less than 1 day. Due to these weaknesses, DES was developed to produce a standard known as Triple DES.

ATM Security

In ATM security systems generally use a PIN number with a combination of four digits. The process of making the PIN number uses the following calculation:

1. Take the last five digits of the account number
2. Combine these five numbers with 11 digits of validation data (validation data created by myself)
3. The sixteen numbers are the data that becomes the input data for the DES algorithm. In processing with the DES algorithm, a 16-digit key is used which is then referred to as a "PIN key".
4. From the results of processing with DES, the first 4 digits are taken and then converted into decimal form - the use of DES will produce numbers with hexadecimal units. These four digits are then referred to as the “natural PIN”.
5. From the natural PIN, 4 digits are added which are referred to as offsets to produce a PIN number that will be used by the customer.

Attack On ATM Security

The use of encryption techniques (cryptography) does not always guarantee one hundred percent of the ATM security system. Various crimes or fraud against the ATM security system is not small. The crimes that occurred ranged from fairly simple actions, such as pickpocketing, mugging, or robbery, to the use of quite sophisticated technology, namely the use of technology to find out account numbers, customer PINs, or duplicate customer security data. The following will explain some of the security threats to the use of ATMs.

Money theft

One of the simplest forms of cheating at an ATM is to steal money from the customer's withdrawal. Of course the theft here is not by pointing the customer after making a transaction but using a money "storage" device that is attached to an ATM machine. Money "depositor" The tool used in this method is a "duplicate" where the money is issued at the ATM machine. Thus, customers who are about to make transactions do not suspect the trap. When a customer makes a transaction, of course, it is expected that the money will come out of the ATM machine. However, because the money is stored in the trap, as if the process that occurred was the ATM machine running out of money, there was no longer any width of money left in the ATM machine. After feeling the transaction process failed, the customer (the victim) left the ATM machine and not long after that the criminals took their "savings" at the ATM.

Card theft

The card theft process referred to here is to use a device that is "embedded" into the ATM machine, namely in the hole/slot to insert an ATM card. actually his ATM card had been stolen. When the customer (the victim) is confused by the situation, the perpetrator seems to come to help and asks the customer to enter the PIN number again under the pretext of confirming the process at the ATM; the criminals secretly peek at the customer's PIN number. Because the ATM card cannot be saved, the customer is advised to report it to the relevant party. After the customer leaves the criminal can make transactions with the card "stored" in the ATM machine and he also knows the PIN number of the card. By using the card theft method, of course, the main concern for criminals is regarding the PIN number of the ATM card so that it can be used. If you use the method previously mentioned, it can certainly raise suspicion for the victim. Therefore, there are several other techniques used to obtain PIN numbers from customers who are victims of the crime, namely: Using hidden cameras This technique is a simple technique. By placing the camera in a strategic and well-hidden place, criminals can easily see the PIN number entered by the customer (the victim). electronic data recording at the ATM machine. By tapping the data access, it is possible to retrieve important data stored in the ATM machine, one of which is the customer's PIN number.

Skimming

The skimming method can be understood as a method of "filtering" data on a customer's ATM card. For crime cases using the skimming method, a tool called a “skimer” is used (figure 14). The function of this tool is to "filter" the data contained in the customer's ATM card. The placement of the skimer is placed around the ATM machine so that it looks as if the device is part of the ATM machine. The way this tool works is by copying the data that is on the magnetic tape of the ATM card when it is swiped on the device. After the data in the ATM card is copied, the criminal can duplicate the ATM card and make money withdrawal transactions at the ATM like a customer.

Phishing

Phishing is a form of crime using social engineering techniques. In using this technique, the perpetrator tries to find out and retrieve the customer's personal data by positioning himself as a person or institution that can be trusted in conducting transactions or communicating electronically. Generally, the use of this fraudulent technique is carried out using the internet, email, or telephone. The perpetrator will claim to be a person who can be

trusted in carrying out a certain activity or transaction. In the form of attacks using ATMs, currently generally using transfer facilities that can be done through ATM machines. By using the account number of a certain destination, the transfer process is carried out and at that time the customer data can be known by the perpetrators of the crime. In the process of communication using a computer network, of course, information about the sender and receiver is needed. By placing himself as the recipient, the perpetrator of the crime can certainly find out data about the sender, in this case the customer (the victim). By using this method, criminals will find out data from customers, especially those related to accounts, addresses, or other related data. The phishing technique carried out with ATM media is to find out the data contained in the magnetic tape (track 2) because on the magnetic tape stored customer account or financial data including card verification value (CVV) and card validation code (CVC). The two data are data used by Visa and MasterCard which are data for making transactions. By getting this data, the perpetrator can duplicate the card and use the card in daily transactions without worrying about having a sufficient balance or not. If the card can no longer be used, then what is done is to use another card belonging to another customer.

Generally, attacks using phishing techniques are currently quite a lot happening on the internet media, one of which is in the banking sector with internet banking services. Through this service, customers can perform banking transactions such as fund transfers, payments, and so on. The use of techniques with internet media is generally carried out on users of financial services. For certain services that are available using internet media, personal data from users is required. For example, for a business activity, call it a fund transfer. With online services, it will certainly make it easier for customers to carry out their transactions. Customers no longer need to come to the bank just to make a fund transfer transaction.

On this occasion a phisher (phishing perpetrators) carry out the action. By creating a web page that resembles a web page from a bank, phishers disguise themselves and act like the bank. To process transactions, of course, you need personal data including account numbers, identity numbers, contact numbers, and so on. Of course, without being suspicious, customers provide the data that is "needed". Thus, the phisher has found the "fish" he was looking for. Indirectly, the phisher already has the data needed to find out what benefits he can get from the victim.

The danger posed by the criminal act of phishing is not only technologically detrimental but can also have an impact on the social environment. The main loss will certainly be experienced by the banking sector because the criminal act in addition to eliminating assets and wealth also results in a loss of public trust. In terms of social impact, of course, this phishing act is very influential, especially related to personal security (privacy). Therefore, improving data security is a major concern in handling this case.

METHOD

Method of collecting data

Data Collection Method Primary data collection method was carried out by distributing questionnaires through google forms to obtain data. In this study, researchers used a Likert Scale. The Likert scale is a psychometric scale that is most widely used in research in the form of surveys. This scale is named after Rensis Likert, who published a report describing the use of this scale. When responding to questions on a Likert scale, respondents determine their level of agreement with a statement by choosing one of the available options. Usually five scale options are provided with a format such as: 1 = Strongly Disagree, 2 = Disagree, 3 = Doubtful, 4 = Disagree, 5 = Strongly Disagree.

To get data that is ordinal and scored as follows:

Table 1. Likert Score

PK	STS	TS	RR	S	SS
	1	2	3	4	5

Description :
PK : Questionnaire Question STS : Strongly Disagree TS : Disagree RR : Doubt S : Agree SS : Strongly Agree

RESULTS AND DISCUSSION

In this study, researchers distributed questionnaires to lecturers, staff employees, and students at Manado State University which contained 5 questions that represented the five aspects using google forms media. Users fill out a questionnaire that has been distributed based on their experience (what they see and feel) when using an ATM Machine d. Each question from the questionnaire has a purpose to measure the level according to user acceptance, which will then be assessed using a Likert scale. These questions have represented the five aspects, including learnability, efficiency, memorability, errors, and satisfaction. From the questionnaires that have been given to the respondents, the data were analyzed using a Likert scale model.

Index Formula % = Score / Y x 100

Y = The highest score likert x number of respondents (Highest Number 5) "Pay attention to the weight of the score"

X = The lowest score likert x number of respondents (Lowest Number 1) "Pay attention to the weight of scores"

Table 2. Answer

Answer	Description
0% - 19.99 %	Strongly Disagree
20% - 39.99 %	Disagree
40% - 59.99%	Doubt
60% - 79.99%	Agree
80% - 100%	Strongly Agree

Analysis After distributing the questionnaires given to 30 respondents, then a recap is made of the results of the questionnaires obtained.

Table 3. Answer Recapitulation

No	Question	Value Percentage	Description
1.	Making Transactions with ATM	86 %	Strongly Agree
2.	Faster process with ATM	79,3 %	Agree
3.	ATM makes transactions between banks easy	80 %	Strongly Agree
4.	ATM is safe to make transactions	81,3 %	Strongly Agree
5.	There are many crimes and carding counterfeits at ATM	83,3 %	Strongly Agree

Table 3 above shows the value of user satisfaction/acceptance (acceptance) to each question asked. It can be seen that the ATM security system has a percentage value. on the Likert scale. This means that the ATM security system is easily recognized by the user in terms of the interface. If it is adjusted to the ATM security system, the data says that the ATM security system has a very good value. This is indicated by the value of the results on the five attributes as follows: The value of the attribute "Conducting Transactions with ATM" is 86% which

indicates that Android already has the value of the Learnability aspect. The value of the attribute "Process is faster with ATM" of 79.3% indicates that Android already has an Efficiency aspect value. The attribute value "ATM makes inter-bank transactions easier" by 80% indicates that Android already has a Memorability aspect value. The attribute value of "ATM is safe for making transactions" of 81.3% and the attribute of "Easy to understand image symbols" of 74% makes Android can be said to have minimized the Errors aspect. And from all the attributes that have an average value above 3, it shows that the ATM security system has a good Satisfaction aspect.

CONCLUSION

ATM (Automated Teller Machine / Automated Teller Machine) is a computerized device used by a financial institution (bank) in an effort to provide financial transaction services (withdrawing money) in public places without the need for bank employees (tellers). The use of ATMs has expanded beyond just withdrawing money. It is now possible for customers to make money transfers, payments, balance checks, and other financial transactions simply by using an ATM. In general, ATM technology is a form of distributed computer network. ATM network The existence of transaction processing (communication) between computers through a wide network, the issue of security is an issue that needs special attention. This is of course to ensure that the transaction process can occur properly and correctly. The security technique used.

REFERENCES

Al-Thani, S. F. (2017). *The Security of The ATM Machines in Relation to Students* (Doctoral dissertation, Cardiff Metropolitan University).

Adeka, M., Shepherd, S., & Abd-Alhameed, R. (2013). Password Security Awareness in African Countries within the Context of Password Security Purgatory.

Adhikari, M. K. (2018). *Cyber Security Awareness Level in Teenage Group of Nepal* (Doctoral dissertation, Central Department of Mathematics and ICT Education).

Adepoju, S. A., & Alhassan, M. E. (2010). Challenges of automated teller machine (ATM) usage and fraud occurrences in Nigeria–A case study of selected banks in Minna Metropolis.

Chaudhari, A., Patil, M., & Sonawane, M. (2014). A Study on Awareness of E-Banking Services in College Students of Bhusawal City. *International Journal of Innovative Research & Development*, *3*(1), 219-224.

Csermely, P. (2007). Information security studying by means of extracurricular research projects. *Science Education: Models and Networking of Student Research Training Under 21*, *16*, 286.

Gardner, B., & Thomas, V. (2014). *Building an information security awareness program: Defending against social engineering and technical threats*. Elsevier.

Katono, I. W. (2011). Student evaluation of e-service quality criteria in Uganda: the case of automatic teller machines. *International Journal of Emerging Markets*.

Mustafa, S., Warraich, U. A., Khan, B. S., & Shaikh, K. A. (2015). assessing the Level of information security awareness Displayed by administrative and Operational staff of Banking sector. *Journal of Business strategies*, *9*(1), 31.

Olatokun, W. M., & Igbinedion, L. J. (2009). The adoption of automatic teller machines in Nigeria: An application of the theory of diffusion of innovation. *Issues in Informing Science & Information Technology*, *6*.

von Solms, R., & Warren, M. (2011). Towards the human information security firewall. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *1*(2), 10-17.

Walaza, M., Loock, M., & Kritzinger, E. (2017). A framework to integrate information and communication technology security awareness into the south african education system. *University of South Africa*.